UNIVERSITY OF PRIMORSKA

FACULTY OF MATHEMATICS, NATURAL SCIENCES
AND INFORMATION TECHNOLOGIES

Master's Study Programme Mathematical Sciences
Second Bologna cycle

Anna Klymenko

Multiply transitive permutation groups via the small Mathieu groups

Master Thesis

Supervisor: assoc. prof. István Kovács

Koper, 2012

KEY WORDS DOCUMENTATION

Name and last name: Anna Klymenko

Title of master thesis: Multiply transitive permutation groups via the small Mathieu groups

Place: Koper

Year: 2012

No. of pages: 55 No. of figures: 11 No. of tables: 1

No. of references: 21

Supervisor: assoc. prof. István Kovács

UDC: 512.542.7(043.2)

Keywords: permutation group, group action, orbit, stabilizer, multiply transitive group, affine group, Mathieu group

Math. Subj. Class. (2010): 20B05, 20B20, 20B25, 05B07, 05E18

Abstract: A permutation group G acting on a set Ω is k-transitive if any k-tuple of distinct points can be mapped, by some element of G, to any other k-tuple of distinct points. A group is called multiply transitive if it is at least 2-transitive. Examples of multiply transitive groups include the symmetric groups, the alternating groups, the affine groups, the projective groups and the Mathieu groups. In this master thesis we review first the basic properties of multiply transitive permutation groups, describe their extensions

and give several examples. The main part of the thesis is Section 5, where we construct the Mathieu groups M_{11} and M_{12} by working out the assignments 1.9.1 – 1.9.11 of the book N. L. Biggs and A. T. White: *Permutations groups and combinatorial structures*, London Math. Soc. Lecture Notes Series **33**, Cambridge University Press, Cambridge 1979 (1.9 Project: Some multiply transitive groups, pages 21-23). Also, we check the most important properties of the constructed permutation groups such as transitivity, primitivity and simplicity. In this paper we try to show how useful could be multiply transitive groups, that is why we have present a bunch of its applications.

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Ime in priimek: Anna Klymenko

Naslov: Večkratno-tranzitivne permutacijske grupe glede na majhne Mathieujeve grupe

Kraj: Koper

Leto: 2012

Število listov: 55 Število slik: 11 Število tabel: 1

Število referenc: 21

Mentor: izr. prof. dr. István Kovács

UDK: 512.542.7(043.2)

Ključne besede: permutacijska grupa, delovanje grupe, orbita, stabilizator, večkratno-tranzitivna grupa, afina grupa, Mathieujeva grupa

Math. Subj. Class. (2010): 20B05, 20B20, 20B25, 05B07, 05E18

Izvleček: Za permutacijsko grupo G pravimo, da deluje na množici Ω k-tranzitivno, če vsako k-terico različnih točk lahko, z nekim elementom iz G, preslikamo v poljubno drugo k-terico različnih točk. Grupa je večkratno-tranzitivna, če je vsaj 2-tranzitivna. Nekatere grupe seznama večkratno-tranzitivnih grup so simetrične grupe, alternirajoče grupe, afine grupe, projektivne grupe in Mathieujeve grupe. V tem magistrskem delu najprej pregledamo osnovne lastnosti večkratno tranzitivnih permutacijskih grup, opišemo njihove razširitve in podamo številne primere. Glavni del magistrskega dela je 5. poglavje,

v katerem konstruiramo Mathieujevi grupi M_{11} in M_{12} preko vaj 1.9.1 - 1.9.11 knjige N. L. Biggs in A. T. White: *Permutations groups and combinatorial structures*, London Math. Soc. Lecture Notes Series **33**, Cambridge University Press, Cambridge 1979 (1.9 Project: Some multiply transitive groups, pages 21-23). Poleg tega raziščemo najpomembnejše lastnosti konstruiranih permutacijskih grup, kot so tranzitivnost, primitivnost in enostavnost. V tem delu skušamo pokazati kako uporabne so lahko večkratno-tranzitivne grupe, zato pokažemo kopico njihovih konkretnih uporab.

Contents

List of figures

List of tables

Symbols and abbreviations

$\lvert G \rvert$	the order of the group G
(G,Ω) or $G \times \Omega$	group G acts on the set Ω
$Sym(\Omega)$, S_n	symmetric group of a set Ω, of a set of n symbols
$Alt(\Omega)$ or A_n	alternating group of a set Ω, of a set of n symbols
$Orb(\alpha)$ or α^G	orbit of the element α under the action of G
$Stab_G(\alpha)$ or G_α	stabilizer of the element α under the action of G
$r(G)$	the rank of a transitive permutation group G
$AGL_d(F)$	the d-dimensional affine group over the field F
M_{10}, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}	the Mathieu groups of degree 10, 11, 12, 22, 23 and 24, respectively
$S(\Omega,B)$ or $S(t,k,v)$	a Steiner system under the set Ω

Acknowledgements

I would like to thank my mentor assoc. prof. István Kovács for all the help, patience and encouragement during the work under the master thesis. Sincere and big thanks to my family and especially to Aleksey Masalitin for all their support and trusteeship.

Chapter 1

INTRODUCTION

In light of the extensive investigations of the combinatorial and geometrical structures multiply transitive groups became very popular. Their structure underpins many interesting mathematical objects such as the Witt designs, Golay codes and Leech Lattice [7]. Even outside of pure mathematics, we can find interesting applications of multiply transitive groups, for example in music [17] or even for creation of new puzzles [10]. The interest to this topic has started from the question as which groups besides symmetric and alternating could be multiply transitive? One type of such groups has been found in 1860 by Emile Mathieu, when he published an article about 4- and 5-transitive groups and in the 1930's Ernst Witt proved that this groups are also simple. They were first in the list of simple sporadic groups. In our work we explore Mathieu groups like good examples of multiply transitive groups.

The aim of this thesis is to construct and investigate the main properties of the Mathieu groups of small degree. For the construction we use the method of one-point extension, and then we investigate properties of these groups using simplicity criteria or a theorem which gives us an upper bound of transitivity of this group.

Our work consist of five chapters:

The first chapter is an introduction to the master thesis.
The second chapter "Basic concept of multiply transitive groups" is a brief introduction to the theory of permutation group. The section "Basic definitions" gives necessary infor-

mation from the general theory, which will be used latter. The second section "Multiply transitive groups" introduces the concept of a multiply transitive group.

The third chapter "Construction and properties of multiply transitive groups" gives us a method for this thesis. In the section "Extensions of multiply transitive groups" it is shown how to construct multiply transitive groups. The second section "Primitivity of the multiply transitive groups" gives some theorems which could help to determine if a group is primitive on a set. And the last section "Simplicity of the multiply transitive groups" presents criteria of simplicity for multiply transitive groups. We try to be careful with references and chose the best classical literature for the first and the second chapters of our thesis, such us [18, 8, 21].

In the forth "Examples and applications of multiply transitive groups" we first recall the classification of all multiply transitive groups and then give more details in the special cases of the affine groups and the Mathieu groups. Here we also give a couple of examples and applications of multiply transitive groups.

The last chapter "The construction of the Mathieu groups M_{10}, M_{11} and M_{12}" is the main part of the thesis where we construct the Mathieu groups M_{10}, M_{11} and M_{12} by working out the assignments 1.9.1 - 1.9.10 and 1.9.11 of the book N. L. Biggs and A. T. White: *Permutations groups and combinatorial structures*, London Math. Soc. Lecture Notes Series **33**, Cambridge University Press, Cambridge 1979 (1.9 Project: Some multiply transitive groups, pages 21-23). Finally, we check the most important properties of the constructed permutation groups such as transitivity, primitivity and simplicity.

Chapter 2

BASIC CONCEPT OF MULTIPLY TRANSITIVE GROUPS

For the beginning let us review some definitions and theorems from the theory of permutation groups, which will be needed later. Then we will present concept of a multiply transitive group.

2.1 BASIC DEFINITIONS

In this section we would like to give all necessary information from the theory of permutation groups. We have used such source of information like [1, 13, 18].

Definition 2.1 *A bijection (a one-to-one, onto mapping) of* Ω *onto itself is called a permutation of* Ω.

Example. Let us consider set $S = \{1, 2, 3, 4, 5, 6, 7\}$, then permutation of S will be

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 5 & 2 & 7 & 6 \end{pmatrix},$$

the scheme of permutation is on Figure 2.1.

The set of all permutations of Ω forms a group, under composition of mappings, called

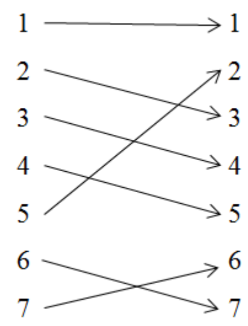

Figure 2.1: The example of a permutation

the symmetric group of Ω. We will denote it like $Sym(\Omega)$ or S_n, where $|\Omega| = n$. The group of all even permutations of Ω is called the alternating group $Alt(\Omega)$ or A_n.

Definition 2.2 *A permutation group is just a subgroup G of the symmetric group $Sym(\Omega)$.*

Definition 2.3 *Let G be a group and Ω be a nonempty set, and suppose that for each $\alpha \in \Omega$ and for each $g \in G$ we have defined an element of Ω denoted by α^g (in other words, $(\alpha, g) \mapsto \alpha^g$ is a function from $\Omega \times G$ into Ω). Then we say that this defines an action of G on Ω (or G acts on Ω or short notation (G, Ω) or $G \times \Omega$) if we have:*

- *$\alpha^{id} = \alpha$ for all $\alpha \in \Omega$ (where id denotes the identity element of G);*
- *$(\alpha^x)^y = \alpha^{xy}$ for all $\alpha \in \Omega$ and all $x, y \in G$.*

Example. One of the classical example of group action is the dihedral group D_8 which acts on the vertices of a rectangle (Figure 2.2). The elements of the dihedral group are all symmetries of the rectangle:

$$D_8 = \{id, (1234), (1432), (13)(24), (12)(34), (14)(23), (13), (24)\}.$$

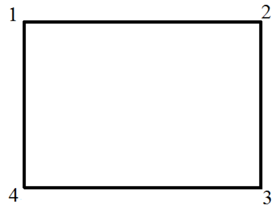

Figure 2.2: Rectangle

Definition 2.4 *The homomorphism $\phi : G \to Sym(\Omega)$, given by $\phi(g) = g^{\alpha}$ will be called a permutation representation of G on Ω.*

Definition 2.5 *Let π be a permutation representation of G on Ω. When $Ker(\pi) = \{id\}$ we say that the representation is faithful; in this case it is convenient to identify G with its image in $Sym(\Omega)$, so we recover the case of a permutation group $\Omega \times G$.*

Definition 2.6 *Orbit of the element $\alpha \in \Omega$ under the action of a group G is*

$$Orb(\alpha) = \{\alpha^g : g \in G\}$$

Definition 2.7 *The set of elements in G which fix an element $\alpha \in \Omega$ will be called the stabilizer of α in G and is denoted by*

$$Stab_G(\alpha) = \{g \in G : \alpha^g = \alpha\}.$$

Suppose $\Delta \subseteq \Omega$, such that $\Delta = \{\alpha_1, \cdots, \alpha_n\}$. Then the pointwise stabilizer of Δ in G is

$$Stab_G(\alpha_1, \cdots, \alpha_n) = \{g \in G : \alpha^g = \alpha, \alpha \in \Delta\}$$

and the setwise stabilizer of Δ in G is

$$Stab_G(\Delta) = \{g \in G : \Delta^g = \Delta\}.$$

Theorem 2.8 *(The Orbit-Stabilizer Lemma).*

$$|G| = |Stab_G(\alpha)| \cdot |Orb(\alpha)| \text{ for all } \alpha \in \Omega.$$

Proof. We determine the length $|Orb(\alpha)|$ of orbit $Orb(\alpha)$.
We have $\alpha^h = \alpha^r$ if and only if $hr^{-1} \in Stab_G(\alpha)$, i.e. $h \in Stab_G(\alpha)r$. Therefore there are precisely as many points α^h as there are distinct right cosets $Stab_G(\alpha)r$. However, this number is $|G : Stab_G(\alpha)|$ and therefore

$$|Orb(\alpha)| = |G| : |Stab_G(\alpha)|,$$

as asserted. □

Definition 2.9 *A group G is acting on a set Ω is said to be transitive on Ω if it has only one orbit, and so $Orb(\alpha) = \Omega$ for all $\alpha \in \Omega$ or equivalently we could say that G is transitive if for every pair of points $\alpha, \beta \in \Omega$ there exist $g \in G$ such that $\alpha^g = \beta$.*
A group which is not transitive is called intransitive.

Definition 2.10 *[1] A group G acting transitively on a set Ω is said to act regularly if $Stab_G(a) = \{id\}$ for each $\alpha \in \Omega$,and then $|G| = |\Omega|$.*

Proposition 2.11 *Suppose that G is transitive in its action on the set Ω. Then:*

(i) $|\Omega|$ divides $|G|$;

(ii) The stabilizers $Stab_G(\alpha)$, $\alpha \in \Omega$ form a single conjugacy class of subgroups of G.

Proof. For (i) the Orbit-Stabilizer Lemma gives us $|G| = |Orb(\alpha)| \cdot |Stab_G(\alpha)|$, but since G acts transitively, $Orb(\alpha) = \Omega$ for every $\alpha \in \Omega$, hence $|G| = |\Omega| \cdot |Stab_G(\alpha)|$, hence $|Stab_G(\alpha)| = \frac{|G|}{|\Omega|}$, and so $|\Omega|$ divides $|G|$.

Let us prove (ii) by definition. We should show that

$$g^{-1}Stab_G(\alpha)g = Stab_G(\beta)$$

where $\alpha, \beta \in \Omega$. Then:

$$\begin{aligned} g^{-1}Stab_G(\alpha)g &= \{g^{-1}hg : \beta^{(g^{-1}hg)} = (\alpha^g)^{(g^{-1}hg)} = \alpha^{hg} = \beta\} \\ &= \{h' : \beta^{h'} = \beta\} = Stab_G(\beta). \end{aligned}$$

□

Definition 2.12 *A subset $\Delta \subseteq \Omega$ is called a block of G if for any $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. Obviously, Ω itself, $\emptyset$ and all singleton subset $\{\alpha\}$ are blocks of G, which are called the trivial blocks.*

Definition 2.13 *Let G acts on Ω transitively. If G does not have any nontrivial blocks, then G is called a primitive group. Otherwise, it is called imprimitive.*

Proposition 2.14 *[13, Proposition 6.1.4] Let $G \leq Sym(\Omega)$ be a transitive group and let $r(\alpha)$ denote the number of orbits of stabilizer $Stab_G(\alpha)$ on Ω. Then*

$$r(\alpha) = \frac{1}{|G|} \sum_{g \in G} |fix_\Omega(g)|^2.$$

It follows from the above proposition that if $G \leq Sym(\Omega)$ is transitive, then for $\alpha \in \Omega$ the number of orbits $r(\alpha)$ of $Stab_G(\alpha)$ does not depend on the choice of α. This number is called the rank of G and denoted by $r(G)$.

2.2 MULTIPLY TRANSITIVE GROUPS

Definition 2.15 *The permutation group $G \times \Omega = (G, \Omega)$ is k-transitive ($k \geq 1$) if given any two ordered k-tuples $(\alpha_1, \dots, \alpha_k)$, $(\beta_1, \dots, \beta_k)$ of distinct elements of Ω, then there exist some $g \in G$ such that*

$$\alpha_i^g = \beta_i,\ 1 \leq i \leq k.$$

Clearly, a k-transitive group is also l-transitive for $1 \leq l \leq k$. Usually, when we say that G is k-transitive on Ω we mean that k is the largest integer for which this is so. The determination and construction of multiply transitive groups is facilitated by the following lemma.

Lemma 2.16 *[1, Lemma 1.3.6] Suppose that G is known to be transitive on Ω. Then G is k-transitively on Ω if and only if $Stab_G(\alpha)$ acts $(k-1)$-transitive on $\Omega \setminus \{\alpha\}$.*

Proof. Let us suppose first that $Stab_G(\alpha)$ is $(k-1)$-transitive on $\Omega \setminus \{\alpha\}$. Given any ordered k-tuples $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$ of distinct elements of Ω, we may select $g_1, g_2 \in G$ and $h \in Stab_G(\alpha)$ with the properties

$$g_1(\alpha_1) = \alpha, \;\; g_2(\beta_1) = \alpha,$$

$$h[g_1(\alpha_i)] = g_2(\beta_i), \;\; 2 \leq i \leq k.$$

Then $g_2^{-1} h g_1$ is an element of G transforming the ordered k-tuples as required.

The converse is straightforward. □

If we apply repeatedly the Orbit-Stabilizer Lemma for a 2-transitive group, we get the following formula:

$$|G| = n(n-1)(n-2)\ldots(n-k+1)|Stab_G(\alpha_1, \alpha_2, \ldots, \alpha_k)|$$

where $Stab_G(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is the pointwise stabilizer of $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$.

Definition 2.17 *[8] A k-transitive group G is called sharply k-transitive if the identity element is the only permutation fixing k points.*

If G is sharply k-transitive and $g_1, g_2 \in G$ are such elements that $g_1 \neq g_2$ and $\alpha_i^{g_1} = \alpha_i^{g_2} = \beta$, $1 \leq i \leq k$, then $g_1 g_2^{-1} \in Stab_G(\alpha_1, \ldots, \alpha_k)$ and $g_1 g_2^{-1} = id$. It is easy to see that there exists a one-to-one correspondence between ordered sets $(\beta_1, \ldots, \beta_k)$ and permutations in G, namely:

$$(\beta_1, \ldots, \beta_k) \leftrightarrow \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_k \cdots \\ \beta_1 & \beta_2 & \cdots & \beta_k \cdots \end{pmatrix}$$

Thus $|G| = n(n-1)\ldots(n-k+1)$.

Theorem 2.18 *[1, Theorem 1.3.8] The symmetric group $Sym(\Omega)$ is sharply n-transitive, and $Alt(\Omega)$ is sharply (n-2)-transitive in their actions on the set $\Omega = \{1, 2, 3, \cdots, n\}$, $n \geq 3$.*

Proof. The first part is obvious, since $Sym(\Omega)$ contains all permutations of the n-set. In the alternating case, we may proceed by induction. When $n = 3$, A_3 contains (123) and so it is 1-transitive. The stabilizer of the symbol n in $Alt(\Omega) = Alt(n)$ is $Alt(n-1)$ and so by lemma 1.17 the induction step is valid. It remains to be shown that $Alt(n)$ cannot be more than (n-2)-transitive. To see this, we remark that the only permutation of $1, 2, 3, \ldots, n$ which takes the ordered (n-1)-tuple $(1, 2, \ldots, n-2, n-1)$ to $(1, 2, \ldots, n-2, n)$ is the odd permutation $(n-1, n)$, which is not in $Alt(n)$. Thus $Alt(n)$ is not (n-1)-transitive. □

For any permutation group $G \leq Sym(\Omega)$, if $\alpha^g = \alpha^{g'}$ for $g, g' \in G$, then $g' \in Stab_G(\alpha)g$. Thus the right coset $Stab_G(\alpha)g$ is the set of elements $g' \in G$ which map α to α^g. Hence, if G is transitive, we have a coset decomposition as follows:

$$G = Stab_G(\alpha) \cup (\cup_{\beta \neq \alpha} Stab_G(\alpha) g_\beta),$$

where the second union is taken over all representatives g_β of elements which map α to β.

Theorem 2.19 *Let G be a transitive group on Ω with stabilizer $Stab_G(\alpha)$, $\alpha \in \Omega$. Then G has rank $r(\alpha)$ if and only if G can be decomposed into $r(\alpha)$ distinct double cosets of $Stab_G(\alpha)$. Furthermore if $G = \cup_{i=1}^{r} Stab_G(\alpha) g_i Stab_G(\alpha)$, then the orbits of $Stab_G(\alpha)$ on Ω are*

$$\Delta_i = \{\alpha^g : g \in Stab_G(\alpha) g_i Stab_G(\alpha)\}, \ i = 1, 2, \ldots, r.$$

In particular, G is 2-transitive if and only if for any $g \notin Stab_G(\alpha)$,

$$G = Stab_G(\alpha) \cup Stab_G(\alpha) g Stab_G(\alpha)$$

.

Proof. Let $H = Stab_G(\alpha)$ and let $\alpha_1^H, \alpha_2^H, \dots, \alpha_r^H$ be the r distinct orbits of H on Ω with $\alpha_1 = \alpha$. Since G is transitive, there exist $g_j \in G$ such that $\alpha_i = \alpha^{g_i}$ for each $i = 1, 2, \dots, r$. Then the orbits are

$$\Delta_i = \alpha_i^H = \{\alpha^g : g \in Hg_iH\}, i = \{1, 2, \dots, r\}.$$

Now, if $i \neq j$, then $Hg_iH \cap Hg_jH = \emptyset$ because $\Delta_i \cap \Delta_j = \emptyset$.

Conversely, if $G = \cup_{i=1}^r Hg_iH$ is a decomposition into r distinct double cosets of H, then $\Delta_i = \alpha^{g_iH}$, $i = \{1, 2, \dots, r\}$ are the r distinct orbits of H on Ω. Since G is transitive, we have $\cup_i \Delta_i = \Omega$. We need show that $\Delta_i \neq \Delta_j$ for $i \neq j$. By way of contradiction assume that $i \neq j$ and $\alpha^{g_iH} = \alpha^{g_jH}$. It follows that $\alpha^{g_ih} = \alpha^{g_j}$ for some $h \in H$. Hence $g_ihg_j^{-1} \in H$, and $g_i \in Hg_jH$, which implies $Hg_iH = Hg_jH$, a contradiction.

The last statement is clear because G is 2-transitive if and only if H is transitive on $\Omega \setminus \{\alpha\}$. So, H has two orbits α and $\Omega \setminus \{\alpha\}$. □

Chapter 3

CONSTRUCTION AND PROPERTIES OF MULTIPLY TRANSITIVE GROUPS

3.1 EXTENSION OF MULTIPLY TRANSITIVE GROUPS

Apart from the symmetric and alternating groups, it is not easy to find k-transitive groups for values of k larger than 3; in fact, only two such 4-transitive groups, and two 5-transitive groups are known. A way to construct k-transitive groups is extension of multiply transitive groups [8, 1].

Definition 3.1 *Let group G act on the set Ω transitively, and let $\Omega^+ = \Omega \cup \{*\}$, where $*$ is not a member of Ω. We say that (G^+, Ω^+) is a one-point extension of (G, Ω) if G^+ is transitive on Ω^+ and the stabilizer $(G^+)_* = G$.*

It follows from Lemma 2.17 that if G is k-transitive on Ω, then G^+ is $(k+1)$-transitive on Ω^+. Moreover, if G is sharply k-transitive on Ω, then G^+ is sharply $(k+1)$-transitive on Ω^+.

An obvious example is that S_{n+1} is one-point extension of S_n, the new point $*$ being the symbol $(n+1)$. In order to use construction to define multiply transitive groups, we try

to find a permutation h of Ω^+ such that $G^+ = \langle G, h\rangle$ has the right properties. We should find such h that $*^h$ is still in Ω and G^+ will be transitive. Also we should remember that some h will give us to big G^+ (when $G^+ = S_{n+1}$ or $G^+ = A_{n+1}$), which is not good.
In order to see what additional conditions h must satisfy, we examine the situation when an extension is known to exist. Suppose that H acts on Ω^+ in such way that the stabilizer $H_* = G$ is multiply transitive on Ω, and let α, β be any two distinct points on Ω. Since H is (at least) 3-transitive, there is some $h \in H$ such that h swiches $*$ and α, and fixes β. Also, since G is (at least) 2-transitive there is some g which switches α and β. It follows that both $(gh)^3$ and h^2 fix $*$, and so they belong to G; also, if $f \in G_\alpha$ then hfh fixes $*$ and α, so that $hG_\alpha h = G_\alpha$. We shall show that the existence of h and g, satisfying these condition, is also sufficient for the existence of a one-point extension.

Theorem 3.2 *[1, Theorem 1.5.2] Let (G, Ω) be a k-transitive group with $k \geq 2$ and let $\Omega^+ = \Omega \cup *$. Suppose that we can find a permutation h of Ω^+ and an element $g \in G$ such that*

(i) h switches $*$ and some $\alpha \in \Omega$, $h \in G_\beta$;

(ii) g switches α and β;

(iii) $(gh)^3$ and h^2 are in G;

(iv) $hG_\alpha h = G_\alpha$.

Then the group $G^+ = \langle G, h\rangle$ acts on Ω^+ as a one-point extension of (G, Ω).

Proof. Since G is multiply transitive and $g \notin G_\alpha$, we know from Theorem 2.20 that $G = G_\alpha \cup G_\alpha g G_\alpha$. We shall show that the conditions imply that $\langle G, h\rangle = G \cup GhG$; the result then follows, since nothing in GhG can fix $*$, and so $(G^+)_* = G$. It is sufficient to show that $G \cup GhG$ is a group. To show that $G \cup GhG$ is closed under composition, we need only check that hGh is a subset of $G \cup GhG$, since than we have

$$GhGGhG = G(hGh)G \subseteq G \cup GhG.$$

Now, h^2 fixes α, and $h^2 \in G$, so $h^2 \in G_\alpha$; thus by (iv) $hG_\alpha = G_\alpha h$. Also $(gh)^3 \in G$ so that ghg belongs to

$$(ghg)^{-1}G = g^{-1}h^{-1}G = g^{-1}hG.$$

These remark justify the following calculations:

$$\begin{aligned} hGh &= h(G_\alpha \cup G_\alpha g G_\alpha)h \\ &= hG_\alpha h \cup hG_\alpha g G_\alpha h \\ &= G_\alpha \cup G_\alpha (hgh) G_\alpha \\ &\subseteq G \cup G_\alpha (g^{-1}hG) G_\alpha \subseteq G \cup Ghg, \end{aligned}$$

as required. Thus $G \cup Ghg = \langle G, h \rangle$. □

3.2 PRIMITIVITY OF THE MULTIPLY TRANSITIVE GROUPS

Below we have wrote a few theorems, which determine if a multiply transitive group is primitive. The information was taken from the books [18, 8].

Theorem 3.3 *Every k-transitive* ($k \geq 2$) *group is primitive.*

Proof. Suppose that G is imprimitive, and that Δ is non-trivial block ($|\Delta| \geq 1$) of G. Then there exist three points α, β, γ such that $\alpha, \beta \in \Delta$, $\gamma \notin \Delta$ and $\alpha \neq \beta$. Since G is doubly transitive, the stabilizer $Stab_G(\alpha)$ is transitive on $\Omega \setminus \alpha$. Hence there is a $g \in Stab_G(\alpha)$ such that $\beta^g = \gamma$. Since Δ is block of G and $\alpha^g = \alpha$, we have $\Delta \cap \Delta^g \neq \emptyset$, so $\Delta^g = \Delta$, which contradicts to the fact that $\beta^g = \gamma$. □

The converse of the theorem does not hold in general. For example, the dihedral group D_{2p} for a prime p is primitive but not even 2-transitive.

Theorem 3.4 *Let G acts transitively on the set Ω. Then G is primitive if and only if, for each $\alpha \in \Omega$, the stabilizer G_α is a maximal subgroup.*

Proof. If G_α is not a maximal subgroup, then there is a subgroup H with $G_\alpha < H < G$. We will show that $\alpha^H = \{\alpha^g : g \in H\}$ is nontrivial block; that is G acts imprimitively on the set Ω. If $g \in G$ and $\alpha^H \cap (\alpha^H)^g \neq \emptyset$, then $\alpha^h = (\alpha^{h'})^g$ for $h, h' \in H$. Since $h^{-1}gh'$ fixes α, we have $h^{-1}gh' \in G_\alpha < H$ and so $g \in H$; hence, $(\alpha^H)^g = \alpha^H$, and α^H is a block. It remains to show that α^H is nontrivial. Clearly α^H is nonempty. Choose $g \in G$ with $g \notin H$. If $\alpha^H = \Omega$, then for every $\beta \in \Omega$, there is $h \in H$ with $\alpha^h = \beta$; in particular $\alpha^g = \alpha^h$ for some $h \in H$. Therefore $g^{-1}h \in G_\alpha < H$ and $g \in H$, a contradiction. Finally, if α^H is a singelton, then $H \leq G_\alpha$, contradicting $G_\alpha < H$. Therefore G acts imprimitivly on the set Ω.

Assume that every G_α is a maximal subgroup, yet there exists a nontrivial block B in Ω. Define a subgroup H of G:

$$H = \{g \in G : b^g = B\}.$$

Choose $\alpha \in B$. If $g(\alpha) = \alpha$, then $x \in B \cap B^g$ and so $B^g = B$ (because B is a block); therefore, $G_\alpha \leq H$. Since B is nontrivial, there is $\beta \in B$ with $\alpha \neq \beta$. Transitivity provides $g \in G$ with $\alpha^g = \beta$; hence $\beta \in B \cap B^g$ and so $B^g = B$. Thus, $g \in H$ while $g \in G_\alpha$; that is, $G_\alpha < H$. If $H = G$ then $B^g = B$ for all $g \in G$, and hence $\Omega = B$ by the fact that G acts transitively on the set Ω, contradicting that B is nontrivial. Therefore, $G_\alpha < H < G$ contradicting maximality of G_α. □

3.3 SIMPLICITY OF THE MULTIPLY TRANSITIVE GROUPS

Many of the multiply transitive groups are simple, for example the alternating groups, the projective unimodular groups or Mathieu groups. In this section we will present some simplicity criteria, which will be useful in the practical part of our work. For this section mostly we used [18].

Theorem 3.5 *If Ω is a faithful primitive G-set of degree $n \geq 2$, if $H \lhd G$ and if $H \neq 1$, then Ω is a transitive H-set.*

Proof. The proof of Theorem 3.4 shows that α^H is a block for every $\alpha \in \Omega$. Since Ω is primitive, either $\alpha^H = \emptyset$ (plainly impossible), $\alpha^H = \{\alpha\}$, or $\alpha^H = \Omega$. If $\alpha^H = \{\alpha\}$ for some $\alpha \in \Omega$, then $H \leq G_\alpha$. But if $g \in G$, then normality of H gives $H = g^{-1}Hg \leq g^{-1}G_\alpha g = G_\alpha$. Since Ω is transitive, $H \leq \cap_{\beta\in\Omega} G_\beta = 1$, for Ω is faithful, and this is contradiction. Therefore $\alpha^H = \Omega$ and Ω is transitive H-set. □

Theorem 3.6 *[18, Theorem 9.19] Let group G act faithfully and primitively on the set Ω, and let the stabilizer G_α be a simple group. Then either G is simple or every non-trivial normal subgroup H of G is a regular normal subgroup.*

Proof. If $H \lhd G$ and $H \neq 1$, then by Theorem 3.5 the group H also acts transitively on Ω. We have $H \cap G_\alpha \lhd G_\alpha$ for every $\alpha \in \Omega$, so that simplicity of G_α gives either $H \cap G_\alpha = 1$ and H is regular or $H \cap G_\alpha = G_\alpha$; that is, $G_\alpha \leq H$ for some $\alpha \in \Omega$. Since G_α has to be maximal subgroup of G, so that either $G_\alpha = H$ or $G_\alpha = G$. The first case cannot occur because H acts transitively, so that $H = G$ and G is simple. □

Lemma 3.7 *Let G act transitively on the set Ω and let H be a regular normal subgroup of G. Choose $\alpha \in \Omega$ and let G_α act on $H^* = H \setminus \{id\}$ by conjugation. Then the G_α-sets H^* and $\Omega \setminus \{\alpha\}$ are isomorphic.*

Proof. Let us define

$$f : H^* \to \Omega \setminus \{\alpha\}$$
$$f(h) = \alpha^h$$

If $f(h) = f(k)$ then $h^{-1}k \in H_\alpha = 1$ (by regularity), and so f is injective. Now $|\Omega| = |H|$ (regularity again), $H^* = \Omega \setminus \{\alpha\}$, and so f is surjective. It remains to show that f is a G_α-map. If $g \in G_\alpha$ and $h \in H^*$, denote the conjugate of h by g as h^g. Therefore,

$$f(h^g) = f(g^{-1}hg) = \alpha^{g^{-1}hg} = \alpha^{hg},$$

because $g^{-1} \in G_\alpha$; on the other hand, $f(h)^g = \alpha^{hg}$, and so $f(h^g) = f(h)^g$. □

Lemma 3.8 *Let $k \geq 2$ and let Ω be a k-transitive G-set of degree n. If G has a regular normal subgroup H, then $k \leq 4$. Moreover:*

(i) if $k \geq 2$, then H is an elementary abelian p-group for some prime p and n is a power of p;

(ii) if $k \geq 3$, then either $H \cong Z_3$ and $n = 3$ or H is an elementary abelian 2-group and n is power of 2;

(iii) if $k \geq 4$, then $H \cong V$ (Klein four-group) and $n = 4$.

Proof. We know that G_α-set $\Omega \setminus \{\alpha\}$ is $(k-1)$-transitive for each fixed $\alpha \in \Omega$; by the previous lemma, H^* is $(k-1)$-transitive G_α-set, G_α acts by conjugation.

(i) Since $k \geq 2$, H^* is a transitive G_α-set. The stabilizer G_α acts by conjugation, which is automorphism, so that all elements of H^* have the same (necessarily prime) order p, and H is a group of exponent p. Now $Z(H) \lhd G$, because $Z(H)$ is a nontrivial characteristic subgroup, so that $|\Omega| = |Z(H)| = |H|$, for $Z(H)$ and H are regular normal subgroup of G'(commutator subgroup). Therefore, $Z(H) = H$, H is elementary abelian, and Ω is power of p.

(ii) If $h \in H^*$, then it is easy to see that $\{h, h^{-1}\}$ is a block. If $k \geq 3$, then H^* is a doubly transitive, hence primitive, G_α-set, so that either $\{h, h^{-1}\} = H^*$ or $\{h, h^{-1}\} = \{h\}$. In the first case, $|H| = 3$, $H \cong Z_3$, and $n = 3$. In the second case, h has order 2, and so the prime p in part (i) must be 2.

(iii) If $k \geq 4$, $k-1 \geq 3$ and $|H^*| \geq 3$; it follows that both $H \cong Z_3$ and H_2 are excluded. Therefore, H contains a copy of V; say, $\{1, h, k, hk\}$. Now $(G_\alpha)_h$ acts doubly transitively, hence primitively, on $H^* \setminus \{h\}$. It is easy to see, however, that $\{k, hk\}$ is now a block, and so $H^* \setminus \{h\} = \{k, hk\}$. We conclude that $H = \{1, h, k, hk\} \cong V$ and $n = 4$. Finally, we cannot have $k \geq 5$ because $n \leq 4$. □

Theorem 3.9 *Let Ω be a faithful k-transitive G-set, where $k \geq 2$, and assume that G_α is simple for some $\alpha \in \Omega$.*

(i) If $k \geq 4$, then G is simple.

(ii) If $k \geq 3$ and $|\Omega|$ is not power of 2, then either $G \cong S_3$ or G is simple.

(iii) If $k \geq 2$ and $|\Omega|$ is not prime power, then G is simple.

Proof. By Theorem 3.6, either G is simple or G has a regular normal subgroup H. In the latter case Lemma 3.8 gives $k \leq 4$; moreover, if $k = 4$, then $H \cong V$ and $|\Omega| = 4$. Now the only 4-transitive subgroup of S_4 is S_4 itself, but stabilizer of a point is the nonsimple group S_3. Therefore, no such H exists, and so G must be simple. The other two cases are also easy consequences of Lemma 3.8. □

Chapter 4

EXAMPLES AND APPLICATIONS OF MULTIPLY TRANSITIVE GROUPS

The multiply transitive groups fall into six infinite families, and four classes of sporadic groups. The following list can be found in [19]. Bellow q is a power of a prime number.

1. Certain subgroups of the affine group on a finite vector space, including the affine group itself, are 2-transitive.

2. The projective special linear groups $PSL(d, q)$ are 2-transitive except for the special cases $PSL(2, q)$ with q even, which are actually 3-transitive.

3. The symplectic groups defined over the field of two elements have two distinct actions which are 2-transitive.

4. The field K of q_2 elements has an involution $\sigma(a) = a_q$, so $\sigma_2 = 1$, which allows a Hermitian form to be defined on a vector space on K. The unitary group on V, denoted $U_3(q)$, preserves the isotropic vectors in V. The action of the projective special unitary group $PSU(q)$ is 2-transitive on the isotropic vectors.

5. The Suzuki group of Lie type $S_z(q)$ is the automorphism group of a $S(3, q+1, q^2+1)$, an inversive plane of order q, and its action is 2-transitive.

6. The Ree group of Lie type $R(q)$ is the automorphism group of a $S(2, q+1, q^3+1)$, a unital of order q, and its action is 2-transitive.

7. The projective special linear group $PSL(2, 11)$ has another 2-transitive action related to the Witt geometry W_{11}.

8. The Higman-Sims group HS is 2-transitive.

9. The Conway group C_{O_3} is 2-transitive.

10. The Mathieu groups M_{12} and M_{24} are the only 5-transitive groups besides S_5 and A_7. The groups M_{11} and M_{23} are 4-transitive, and M_{22} is 3-transitive.

In the next two sections we will discuss in more details the affine groups and the Mathieu groups, respectively.

4.1 AFFINE GROUPS

The affine groups arise naturally from affine geometry and can also be defined algebraically. Since the geometry does not enter strongly into the smallest numbers of each family we shall begin with an algebraic introduction to the case of 1-dimensional groups, in which we follow [8].

If the underlying set on which we are acting is a field, then sets of permutations of certain natural types form subgroups of the symmetric group. Historically, these examples of permutation groups arose quite early in the subject; the first examples were given by Évariste Galois in 1830.

Definition 4.1 *Let F be a field. Then it is straightforward to verify that the set A of all permutations of F of the form*

$$t_{\alpha\beta} : \xi \mapsto \alpha\xi + \beta, \;\; \alpha, \beta \in F and \alpha \neq 0$$

constitutes a subgroup of $Sym(F)$ which is called the 1-dimensional affine group over F and is denoted by $AGL_1(F)$.

The higher dimensional affine groups are automorphism groups of affine geometry. The affine geometry $AG_d(F)$ consists of points and affine subspaces constructed from the vector space F^d of row vectors of dimension d over the field F. The points of the geometry are simply the vectors of F^d. The affine subspaces are the translates of the vector subspaces of F^d. Thus if S is a k-dimensional subspace of F^d then

$$S + \beta = \{\alpha + \beta : \alpha \in S\}$$

is an affine subspace of dimension k for every $\beta \in F_d$.
An automorphism of the affine space $AG_d(P)$ is a permutation of the set of points which maps each affine subspace to an affine subspace (of the same dimension). In other words, an affine automorphism is a permutation of the points that preserves, or respects, the affine geometry.

Definition 4.2 *An affine transformation is an affine automorphism of an especially simple form. For each linear transformation $a \in GL_d(P)$ and vector $v \in F_d$ we define the affine transformation $t_{a,v} : F^d \mapsto F^d$ by*

$$t_{a,v} : u \mapsto ua + v.$$

Each of these mappings $t_{a,v}$ is an automorphism of the affine geometry $AG_d(F)$. The set of all $t_{a,v}(a \in GL_d(F), v \in F_d)$ forms the affine group $AGL_d(F)$ of dimension $d \geq 1$ over F. It is easy to verify that $AGL_d(P)$ is a 2-transitive subgroup of $Sym(F)$. The group $AGL_d(F)$ is a split extension of a regular normal subgroup T, consisting of the translations $t_{l,v}$ $(v \in F_d)$ by a subgroup isomorphic to $GL_d(P)$. Since this group has a normal regular subgroups it is not simple and it is primitive, because it is 2-transitive.
Another type of affine automorphism is the permutation of F^d defined by $t_\sigma : u \mapsto u_\sigma$, where $\sigma \in Aut(F)$ and σ acts componentwise on the vector u. All mappings t_σ $(\sigma \in Aut(F))$ form a subgroup of $Sym(F^d)$ isomorphic to $Aut(F)$. This subgroup together with $AGL_d(F)$ generate the group $A\Gamma L_d(F)$ of *affine semilinear transformations*.

4.2 THE MATHIEU GROUPS

Mathieu groups were discovered by French mathematician Emile Mathieu (Figure 4.1) and described in 1861 and 1873 in two papers in the *Journal de Mathematiques Pures et Appliquees* [14, 15].

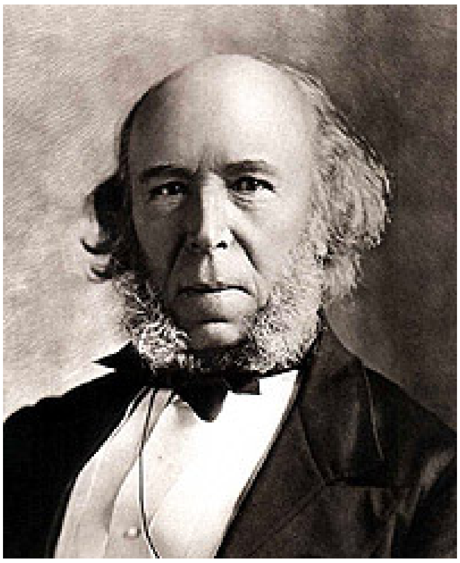

Figure 4.1: Emile Mathieu

The five Mathieu groups, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, are truly remarkable set of finite groups, because they are the first five of the list of 26 sporadic simple groups, and these are the only known finite 4- and 5-transitive groups which are not alternating or symmetric. Moreover, all the five Mathieu groups are subgroups of M_{24}.
The group M_{12} is sharply 5-transitive of degree 12 and its point stabilizer is M_{11}. The group M_{11} in turn is the unique sharply 4-transitive group on 11 points with point stabilizer M_{10}. Some mathematicians do not count M_{10} among the Mathieu groups because it is not simple, but any way it is important to know, that $M_{10} \cong A_6 \cdot 2$.

4.2.1 Steiner System

The Mathieu groups are most simply defined as automorphism groups of certain Steiner systems [8].

Definition 4.3 *A Steiner system $S = S(\Omega, B)$ is a finite set Ω of points together with a set B of subsets of Ω called blocks such that, for some integers k and t, each block in B has size k, and each subset of Ω of size t lies in exactly one block from B.*

We call S an $S(t, k, v)$ Steiner system where $v = |\Omega|$. The parameters are assumed to satisfy $t < k < v$ to eliminate trivial examples. It is important that this use of the term "block" should not be confused with the earlier use in reference to imprimitive groups. Below we give a couple of the nice and classical examples of a Steiner system.

Example. The Fano Plane (Figure 4.2) is an example of an $S(2, 3, 7)$ Steiner System. We have a set Ω of $v = 7$ points, together with a set B of 3-element blocks - represented by 7 lines in the plane. We can see that every pair of points belongs ta a unique line, i.e. every 2-element subset of Ω is in exactly one block as required.

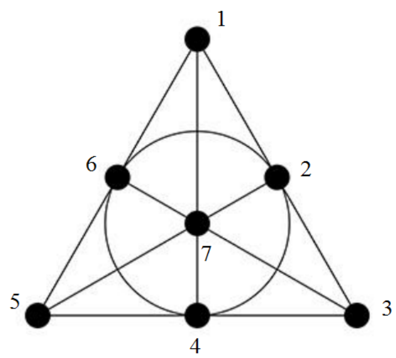

Figure 4.2: The Fano Plane: S(2,3,7)

Example. (Affine space as a Steiner system [8]). Take Ω to be the vector space of dimension d over the field F_q for some prime power q. Take the set B of blocks to be the affine lines of the space, that is, the translates of 1-dimensional subspaces. Then there are $v = q^d$ points in the space and each block has $k = q$ points on it. Any two distinct points are joined by a unique line so lie together in just one block. Thus we have an

$S(2, q, q^d)$ Steiner system. The group $A\Gamma L_d(q)$ (which was present in Section 4.1) is the automorphism group of this Steiner system.

An automorphism of a Steiner system $S(\Omega, B)$ is a permutation of Ω which permutes the blocks among themselves. Many interesting permutation groups, not least the Mathieu groups, arise as automorphism groups of Steiner systems. This gives a means of constructing the groups as well as a concrete tool to study the structure of the groups. The study of Steiner systems and other combinatorial geometries is a lively area of combinatorics that is why the investigation of the Mathieu groups are very needed now.
We complete this section by the list of parameters of Steiner systems which admit the Mathieu groups as their automorphism groups [20].

Table 4.1: The Mathieu groups as automorphism groups of some Steiner Systems

Mathieu group	Steiner system
M_{10}	$S(3, 4, 10)$
M_{11}	$S(4, 5, 11)$
M_{12}	$S(5, 6, 12)$
M_{22}	$S(3, 6, 22)$
M_{23}	$S(4, 7, 23)$
M_{24}	$S(5, 8, 24)$

4.2.2 Other application of the Mathieu groups

In this section we propose to reader to relax a little bit and have some fun with Mathieu groups.

The Mathieu group M_{12} in music

First we would like to present the project of Emma Ross - "Mathematics and Music: The Mathieu Group M_{12}" [17]. She examined how the French composer Oliviér Messiaen (Figure 4.3) used the permutations of M_{12} to compose his music. Specifically she explored the 4^{th} piece of his *Quatre études de rythme* (Four studies in rhythm) titled *Île De Feu 2* (Island of Fire).

Figure 4.3: Olivér Messiaen

The earliest known example of mathematics appearing in musical composition comes from French mathematician and music theorist Marin Marsenne's 1636 work "Harmonie Universelle" where he refers to arranging the order and distribution of notes via simple combinatorial mathematics. It was in the early 20th century when the practice became more popular however. This time saw the revolution of atonal music which inspired the use of new musical scales which, unlike the conventional, featured equal length intervals between each note. Lacking the features of the classic musical scales useful in forming melody and structure, alternative methods for organizing notes into a piece were needed. This opened the door for avant-garde approaches to harmonic organization - the symmetric nature of the scales allowing permutations to be employed in composition. Olivér Messiaen, Igor Stravinsky and Béla Bartók all composed using these innovative compositional notions - avoiding conventional harmonic structure and progression [2].

Emma Ross described in detail how Messiaen applied group theory to writing new compositions. First of all he has numbered the twelve notes in such way like we show on Figure 4.4.

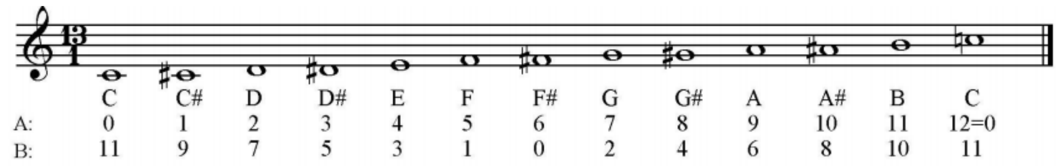

Figure 4.4: Assigning integer labels to each musical note

Assigning numbers to the notes makes spotting the working of modulo 12 arithmetic in the musical scale a much simpler task. Progressing rightwards along the scale in Figure 4.4 the notes become higher in pitch but having reached note 11 we return to 0 in the numbering and start again. This reflects a key property of our musical scale; the note 0 is equivalent to note 12, as well as to note 24 and so on (likewise in the negative direction). Notes equivalent in modulo 12 arithmetic are distinguishable only by pitch - that is note 12 is simply a higher pitched version of 0 while 24 is doubly higher in pitch compared to 0 and so on. It is natural then to consider permutations of these twelve classes of "equivalent" notes and hence the group M_{12}. Numbering the notes as in Figure 4.4, we consider the permutation of a set of 12 integers which generate different orderings of notes to give new melodic phrases. The first labeling shown (A) gives emphasis to the musical convention of considering note C (numbered 0) to be the central note in the scale. The second one (B), looks like random choice by the first glance, but let us check

$$B^{P_O} = \{11, 9, 7, 5, 3, 1, 0, 2, 4, 6, 8, 10\}^{(0,6,9,1,5,3,4,8,10,11)(2,7)} =$$
$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = A,$$

now it is clear that the composer picked such numbering of notes because it is obtain from A by applying P_O^{-1}. We do not know why he did that, but probably it sounds more nice.

To create melody Messiaen uses two permutations $P_O = (0, 6, 9, 1, 5, 3, 4, 8, 10, 11)(27)$ and $P_I = (0, 5, 8, 1, 6, 2, 4, 3, 7, 9, 10)(11)$ (which of course generate whole M_{12}). Diaconis, Graham and Kantor discovered that M12 was generated by P_O ana P_I , this permutations they called *Morgean shuffles* [16]. They can be visualized as follows Figures 4.5 - 4.6 .

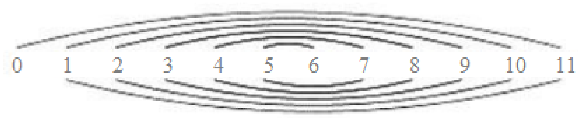

Figure 4.5: Permutation P_O

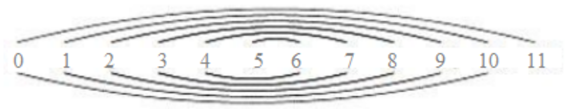

Figure 4.6: Permutation P_I

The Mathueu puzzles M_{12} and M_{24}

Second interesting application of Mathieu groups was described in the article of Igor Kriz and Paul Siegel "Simple groups at play" [10]. The scientists constructed puzzles on the multiply transitive groups M_{12} and M_{24}. Those puzzles, like Rubik's cube, are permutation puzzles. Let us consider these puzzles.

To solve M_{12} puzzle we need a sequence of numbers from 1 to 12, arrange in a row. Only two moves are allowed, but they can be applied any numbers of times in any sequence. The goal of the puzzle is to put the scrambled arrangement back into the ordinary numerical order $(1, 2, 3, ..., 12)$. On Figure 4.7 we have showed the scheme of the work of M_{12} puzzle.

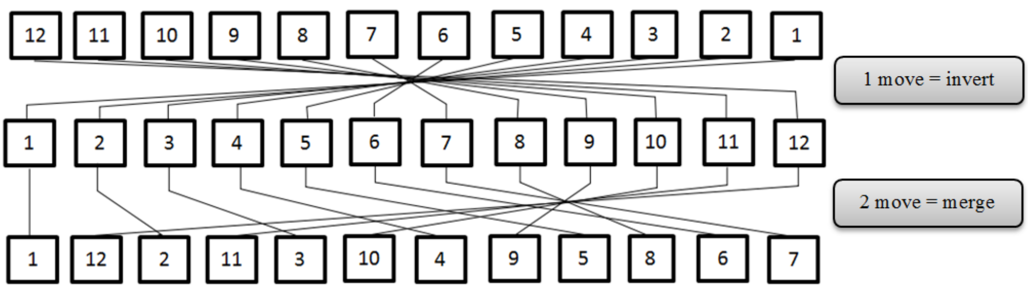

Figure 4.7: The scheme of the work of M_{12} puzzle

The hint of the solution is the fact that the Mathieu group M_{12} is 5-transitive, i.e., it is possible to move any five of the numbers to any five of the 12 positions in the row. Once that is done, all the remaining numbers fall into position; the puzzle is solved. The reason is that the group M_{12} is also sharply 5-transitive, that is why it has $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ or 95040 permutations, which happens to be exactly the number of ways of selecting any five of the 12 numbers and placing each of them somewhere in the sequence. The fact that the entire permutation is specified by fixing the positions of five numbers implies that it is pointless to search for a sequence of moves that would shift only a few numbers, except identity permutation. In other words, every nontrivial sequence of moves must displace at least eight of the twelve numbers. You can find the visualized version of the puzzle on the web-page [11] and Figure 4.8 is one screenshot of it.

Figure 4.8: Computer game of puzzle M_{12}

The second presented puzzle is M_{24} puzzle, which includes 23 numbers arranged in the circle, as if on the face of a clock and a 24^{th} number placed just outside of circle at 12 o'clock (Figure 4.9). As in M_{12} puzzle just two moves are allowed. One move rotates the circle one "notch," sending the number in position 1 to position 2, the number in position 2 to 3, and so forth. The number in position 23 is sent to position 1, and the number outside the circle does not move. The second move simply switches the pairs of numbers that occupy circles having the same color.

Like M_{12}, M_{24} is sharply 5-transitive with some combinations of two moves, it is possible to manipulate the arrangement until any five of the 24 positions. Because of 5-transitivity our hint for solving the M_{12} puzzle helps in solving M_{24} as well: devise moves that return the number 1 through 5 to their proper position without disturbing the numbers already on the places. But this time the solver is not quite done. The group M_{24} has

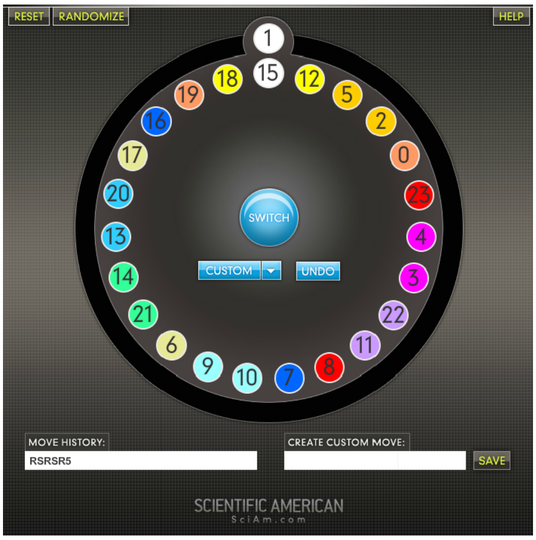

Figure 4.9: Computer game of puzzle M_{24}

$24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ or 244823040 elements; thus, even after the number 1 through 5 are returned to their proper places, the other 19 numbers can still be distributed around the circle in 48 different ways.

Chapter 5

THE CONSTRUCTION OF THE MATHIEU GROUPS $\mathbf{M_{10}}$, $\mathbf{M_{11}}$ AND $\mathbf{M_{12}}$

In this chapter let us apply all knowledge from the earlier part of the thesis to solve the assignments 1.9.1 – 1.9.9 and 1.9.11 from the book [1] and eventually construct the Mathieu groups M_{10}, M_{11} and M_{12}.

When the group G acts on a set Z it also permutes the subsets of Z, and so there are permutation representations of G induced in this way. It is convenient to say that an element $g \in G$ fixes $Y \subseteq Z$ pointwise if $y \in Y$ implies $y^g = y$, and setwise if $y \in Y$ implies $y^g \in Y$. We will construct some multiply transitive groups starting from such a representation. Let $Z = \{a, b, c, d, e, f\}$ and let us write $S_6 = Sym(Z)$. Let X denote the set of the 10 partitions of Z into two three-sets. Label the members of X as follows:

$$\begin{array}{ll} 0 = abc|def & 5 = ace|bdf \\ 1 = abd|cef & 6 = acf|bde \\ 2 = abe|cdf & 7 = ade|bcf \\ 3 = abf|cde & 8 = adf|bce \\ 4 = acd|bef & 9 = aef|bcd. \end{array}$$

Each element $g \in S_6$ induces a permutation of the partitions in X. We denote this permutation by $\hat{g}$, and for any subgroup $G \leq S_6$ write $\hat{G} = \{\hat{g} : g \in G\}$. The mapping $g \mapsto \hat{g}$ defines a permutation representation of S_6 which we denote below by φ.

5.1 SETWISE AND POINTWISE STABILIZERS

Question 5.1 [1, 1.9.1] *Check that φ is a faithful representation and that $\hat{S}_6$ acts transitively on X. Find also the orders of*

(i) the pointwise stabilizer of abc in S_6;

(ii) the setwise stabilizer of abc in S_6;

(iii) the stabilizer of 0 in $\hat{S}_6$.

Solution. Let us check that permutation representation is faithful. By definition, this means that

$$Ker\varphi = \{g \in S_6 : \hat{g} = \hat{id}\} = \{id\}.$$

In fact, the above kernel is the intersection of all stabilizers in $\hat{S}_6$ in this action on X. However, the element $\hat{g} \in \hat{S}_6$ which fixes all elements from the set X must be the identity, so

$$Ker\varphi = \cap_{i=0}^{9} Stab_G(i) = \{\hat{id}\}.$$

Now, we will check if the group $\hat{S}_6$ acts transitive on the set X by finding the orbit $Orb_{\hat{S}_6}(9)$:

$$\begin{aligned}
9^{\widehat{(ab)}} &= 4, \\
9^{\widehat{(acb)}} &= 1, \\
9^{\widehat{(abcd)}} &= 7, \\
9^{\widehat{(cf)}} &= 5, \\
9^{\widehat{(ec)}} &= 6, \\
9^{\widehat{(df)}} &= 7,
\end{aligned}$$

$$\begin{aligned} 9^{\widehat{(ed)}} &= 8, \\ 9^{\widehat{(eb)(cf)}} &= 0, \\ 9^{\widehat{(bf)}} &= 2, \\ 9^{\widehat{(be)}} &= 3, \\ 9^{\widehat{id}} &= 9. \end{aligned}$$

We obtain that $Orb_{\hat{S}_6}(9) = X$, and so $\hat{S}_6$ acts transitively on the set.

We answer next questions (i)-(iii): The pointwise stabilizer of $\{a, b, c\}$ is given as

$$Stab_{S_6}(a, b, c) = \big\{id, (fed), (fde), (df), (de), (fe)\big\};$$

while the setwise stabilizer of $\{a, b, c\}$ is given as

$$\begin{aligned} Stab_{S_6}(\{a, b, c\}) \;\; = \;\; & \big\{id, (fed), (fde), (df), (de), (fe), \\ & (abc), (acb), (ab), (ac), (bc), (abc)(fed), \\ & (abc)(fde), (abc)(df), (abc)(de), (abc)(fe), \\ & (acb)(fed), (acb)(fde), (acb)(df), (acb)(de), (acb)(fe), \\ & (ab)(fed), (ab)(fde), (ab)(df), (ab)(de), (ab)(fe), \\ & (ac)(fed), (ac)(fde), (ac)(df), (ac)(de), (ac)(fe), \\ & (bc)(fed), (bc)(fde), (bc)(df), (bc)(de), (bc)(fe)\big\}. \end{aligned}$$

And so $|Stab_{S_6}(\{a, b, c\})| = 36$.

Since $\hat{S}_6$ acts transitively, we could use the Orbit-Stabilizer Lemma:

$$|\hat{S}_6| = |Orb_{\hat{S}_6}(0)| \cdot |Stab_{\hat{S}_6}(0)|,$$

and from this

$$|Stab_{\hat{S}_6}(0)| = \frac{720}{10} = 72.$$

□

5.2 THE GROUP $\hat{S}_6$ IS 2-TRANSITIVE

Question 5.2 [1, 1.9.2] *By considering $\widehat{(abc)}$ and $\widehat{(def)}$, show that $\hat{S}_6$ is 2-transitive on X.*

Solution. To prove that $\hat{S}_6$ is 2-transitive we should show that $Stab_{\hat{S}_6}(0)$ is transitive on the set $X \setminus \{0\}$. The permutations $\widehat{(abc)}$ and $\widehat{(def)}$ decompose into disjoint cycles as:

$$\widehat{(abc)} = (194)(285)(376) \text{ and } \widehat{(def)} = (123)(456)(798).$$

Now,

$$1^{(194)(285)(376)} = 9 \text{ and } 1^{(123)(456)(798)} = 2.$$

We obtain quickly the following images:

$$1^{\widehat{id}} = 1, \quad 1^{\widehat{(abc)}} = 9, \quad 1^{\widehat{(acb)}} = 4,$$

$$1^{\widehat{(def)}} = 2, \quad 1^{\widehat{(def)(abc)}} = 8, \quad 1^{\widehat{(def)(acb)}} = 5,$$

$$1^{\widehat{(dfe)}} = 3, \quad 1^{\widehat{(dfe)(abc)}} = 7, \quad 1^{\widehat{(dfe)(acb)}} = 6.$$

The stabilizer $Stab_{\hat{S}_6}(0)$ acts transitively on the set $X \setminus \{0\}$, therefore $\hat{S}_6$ acts 2-transitively on the set X.

□

5.3 THE GROUP $\hat{S}_6$ IS NOT 3-TRANSITIVE

Question 5.3 [1, 1.9.3] *How many elements of $\hat{S}_6$ fix both 0 and 1. Find them. Deduce that $\hat{S}_6$ is not 3-transitive on X.*

Solution. Recall that $0 = (abc|def)$ and $1 = (abd|cef)$. Then we can write that $\widehat{(ab)}, \widehat{(ef)} \in Stab_{\hat{S}_6}(0,1)$, and also $\widehat{(ae)(bf)(cd)} \in Stab_{\hat{S}_6}(0,1)$. The last what we should do is to determine the group generated by these elements:

$$\begin{aligned} Stab_{\hat{S}_6}(0,1) &= \big\{\widehat{id}, \widehat{(ab)}, \widehat{(ef)}, \widehat{(ab)(ef)}, \widehat{(afbe)(cd)}, \\ &= \widehat{(aebf)(cd)}, \widehat{(ae)(bf)(cd)}, \widehat{(eb)(af)(cd)}\big\}. \end{aligned}$$

$$|Stab_{\hat{S}_6}(0,1)| = 8.$$

Then

$$\widehat{(ab)} = (49)(58)(67), \quad \widehat{(ef)} = (23)(56)(78), \quad \widehat{(afbe)(cd)} = (2934)(5876),$$

$$\widehat{(aebf)(cd)} = (2439)(5678), \quad \widehat{(ab)(fe)} = (23)(57)(68)(49),$$

$$\widehat{(eb)(af)(cd)} = (24)(39)(68), \quad \widehat{(ae)(bf)(cd)} = (29)(34)(57).$$

We see that the elements in $Stab_{\hat{S}_6}(0,1)$ map 2 to $2,3,4$ or 9. Thus $Stab_{\hat{S}_6}(0,1)$ is not transitive on the set $X \setminus \{0,1\}$, which implies that $\hat{S}_6$ is not 3-transitive on X. □

5.4 THE GROUP $\hat{A}_6$ IS 2-TRANSITIVE

Let $H = \hat{A}_6$ be the group of permutations of X induced by even permutations of Z.

Question 5.4 [1, 1.9.4] *Verify that H is 2-transitive on X and that $Stab_H(0,1)$ is a cyclic group of order 4 generated by $\theta = \widehat{(afbe)(cd)} = (2934)(5876)$.*

Solution. We show first that the group H is transitive on the set X. To show this we calculate the orbit $Orb_H(0)$:

$$
\begin{aligned}
0^{\widehat{(abcde)}} &= (abc|def)^{\widehat{(abcde)}} = (bcd|eaf) = 9,\\
0^{\widehat{(aedcb)}} &= (abc|def)^{\widehat{(aedcb)}} = (aeb|cdf) = 2,\\
0^{\widehat{(cf)(ed)}} &= (abc|def)^{\widehat{(cf)(ed)}} = (abf|dec) = 3,\\
0^{\widehat{(bd)(ef)}} &= (abc|def)^{\widehat{(bd)(ef)}} = (adc|bef) = 4,\\
0^{\widehat{(be)(df)}} &= (abc|def)^{\widehat{(be)(df)}} = (aec|dbf) = 5,\\
0^{\widehat{(bf)(de)}} &= (abc|def)^{\widehat{(bf(de)}} = (afc|deb) = 6,\\
0^{\widehat{(be)(cd)}} &= (abc|def)^{\widehat{(be)(cd)}} = (aed|cbf) = 7,\\
0^{\widehat{(bd)(cf)}} &= (abc|def)^{\widehat{(bd)(cf)}} = (adf|bec) = 8,\\
0^{\widehat{(cd)(ef)}} &= (abc|def)^{\widehat{(cd)(ef)}} = (abd|cef) = 1,\\
0^{\widehat{id}} &= 0.
\end{aligned}
$$

We can conclude that $Orb_H(0) = X$, so H is transitive on the set X.

Observe that, $\widehat{(abc)}$ and $\widehat{(def)} \in H$, then using Section 5.2 we can see that, H is also a 2-transitive group on the set X.

Finally, we find by §5.3 that

$$Stab_H(0,1) = \left\{\widehat{(aebf)(cd)}, \widehat{(afbe)(cd)}, \widehat{(ab)(fe)}, \widehat{id}\right\} \cong Z_4.$$

□

5.5 THE STABILIZER OF 0 IN $\hat{A}_6$

Question 5.5 [1, 1.9.5] *Show that $Stab_H(0)$ is generated by $\theta, \phi_1 = \widehat{(abc)}$ and $\phi_2 = \widehat{(def)}$. Use the fact that H is primitive on X to deduce that H is generated by θ, ϕ_1, ϕ_2, and any element ψ of $H \setminus Stab_H(0)$.*

Solution. We know that H acts transitively on the set X, then by the Orbit-Stabilizer Lemma, $|Stab_H(0)| = 36$. We know that $\widehat{(abc)}$ and $\widehat{(def)}$ are in $Stab_{\hat{S}_6}(0)$, and by §5.4 that $\langle\theta\rangle = Stab_{\hat{A}_6}(0,1)$.

$$\begin{aligned} Stab_H(0) \;=\; &\left\{\widehat{id}, \widehat{(abc)}, \widehat{(def)}, (acb), \widehat{(dfe)},\right. \\ &\widehat{(abc)(def)}, \widehat{(acb)(def)}, \widehat{(abc)(dfe)}, \widehat{(acb)(dfe)}, \\ &\widehat{(afbe)(cd)}, \widehat{(ab)(fe)}, \widehat{(aebf)(cd)}, \\ &\widehat{(ae)(bdcf)}, \widehat{(bf)(adce)}, \widehat{(be)(dafc)}, \widehat{(dbec)(af)}, \\ &\widehat{(dbfc)(ea)}, \widehat{(bdce)(af)}, \widehat{(adcf)(be)}, \widehat{(daec)(fb)}, \\ &\widehat{(df)(ab)}, \widehat{(de)(ab)}, \widehat{(bc)(fe)}, \widehat{(ac)(fe)}, \\ &\widehat{(aebd)(fc)}, \widehat{(aecf)(bd)}, \widehat{(fceb)(ad)}, \widehat{(adfb)(ce)}, \\ &\widehat{(bc)(df)}, \widehat{(bc)(de)}, \widehat{(ac)(df)}, \widehat{(ac)(de)}, \\ &\left.\widehat{(afce)(bd)}, \widehat{(adbe)(fc)}, \widehat{(afbd)(ce)}, \widehat{(cfbe)(ad)}\right\}. \end{aligned}$$

$$|Stab_H(0)| = 36$$

Since H is 2-transitive on X, it must be primitive. This is implies that the stabilizer $Stab_H(0)$ is a maximal subgroup in H, hence $\left\langle Stab_H(0), \psi\right\rangle = H$ for any element $\psi \in H \setminus Stab_H(0)$, and so H is indeed generated by θ, ϕ_1, ϕ_2 and ψ. □

5.6 THE CONSTRUCTION OF THE NEW GROUP M_{10}

Take ψ to be the permutation

$$\psi = \widehat{(ab)(cd)} = (01)(49)(56)(78).$$

Then by Section 5.5, $H = \langle \theta, \phi_1, \phi_2, \psi \rangle$. Define the permutation λ of X, which is not in H, by

$$\lambda = (2735)(4698).$$

Question 5.6 [1, 1.9.6] *Show that the conjugate of each generator of H by λ is an element of H and that $\lambda^2 \in H$. Deduce that there are just two cosets of H in $\langle H, \lambda \rangle$.*

Solution. The generators of H are as follows:

$$\begin{aligned} \theta &= \widehat{(afbe)(cd)} = (2934)(5876), \\ \phi_1 &= \widehat{(abc)} = (194)(285)(376), \\ \phi_2 &= \widehat{(def)} = (123)(456)(798), \\ \psi &= \widehat{(ab)(cd)} = (01)(49)(56)(78). \end{aligned}$$

We obtain their conjugates by λ as

$$\begin{aligned} \lambda\theta\lambda^{-1} &= (2735)(4698)(2934)(5876)(2537)(4896) = (2439)(5678), \\ \lambda\phi_1\lambda^{-1} &= (2735)(4698)(194)(285)(376)(2537)(4896) = (247)(359)(168), \\ \lambda\phi_2\lambda^{-1} &= (2735)(4698)(123)(456)(798)(2537)(4896) = (269)(348)(157), \\ \lambda\psi\lambda^{-1} &= (2735)(4698)(01)(49)(56)(78)(2537)(4896) = (29)(34)(01)(68). \end{aligned}$$

As we know epimorphisms preserve the orders of elements, i.e. images and preimages have the same orders. Using this fact we could show that all conjugates above are in H.

Suppose that $\lambda\theta\lambda^{-1} = \hat{x}$ where $x \in A_6$. Then x is of order 4, thus its cyclic structure must be as $(****)(**)$. We can also use the fact that $\hat{x}$ fixes both 0 and 1. Now, using §5.4, we find that our x is equal to $\widehat{(aebf)(cd)}$.

Step-by-step we will find x also for the permutations ϕ_1, ϕ_2 and ψ. Using the same fact about orders we can see, that $\lambda\phi_1\lambda^{-1} = \hat{x}$ where x could be of cycle structure $(***)$ or $(***)(***)$ and also we know that $\hat{x} \in Stab_H(0)$, then there are only 8 possible x. That is why we easily figure out $x = (acb)(dfe)\hat{}$. In the similar way we have find that $\lambda\phi_2\lambda^{-1} = (acb)(def)\hat{}$. So we can conclude that both elements $\lambda\phi_1\lambda^{-1}$ and $\lambda\phi_2\lambda^{-1}$ is inside A_6. The x of $\lambda\psi\lambda^{-1}$ is equal to element from A_6, which is $(ab)(ef)\hat{}$.

For λ^2 we get that

$$\lambda^2 = (2735)(4698)(2735)(4698) = (23)(57)(49)(68) = (ab)(ef)\hat{}.$$

Now we would like to notice that in group $\langle H, \lambda \rangle$ exist just two cosets of H, they are H and λH, and this follows from the fact that the group H is of index 2 in $\langle H, \lambda \rangle$. □

Definition 5.7 *The group $M_{10} = \langle H, \lambda \rangle$ is called the Mathieu group on* 10 *symbols.*

5.7 THE GROUP M_{10} IS SHARPLY 3-TRANSITIVE

Question 5.8 [1, 1.9.7] *Verify that the Mathieu group M_{10} is sharply 3-transitive on X.*

Solution. By the Definition 2.18 we know that if G is k-transitive, and the identity is the only permutation fixing k points, then G is said to be sharply k-transitive, and its order is exactly

$$|G| = n(n-1)\cdots(n-k+1).$$

Since the order of the group M_{10} is 720, which is exactly $10 \cdot 9 \cdot 8$, it remains to prove that M_{10} is 3-transitive.

We will prove it by Lemma 2.17, in other words we will show that $Stab_{M_{10}}(0,1)$ acts transitively on the set $\Omega \setminus \{0,1\}$. Let us take the elements $\lambda, \theta \in Stab_{M_{10}(0,1)}$ from the previous section. Then λ and θ generate the following elements:

$$\begin{gathered}\langle \lambda, \theta \rangle = \{id, (2735)(4698), (2934)(5876), (2537)(4896), (2439)(5678),\\ (2735)(4698) \cdot (2735)(4698) = (23)(75)(49)(68),\\ (2735)(4698) \cdot (2934)(5876) = (2638)(7459),\\ (2537)(4896) \cdot (2934)(5876) = (2836)(4795), ...\}.\end{gathered}$$

Now we could see that $Stab_{M_{10}}(0,1)$ acts transitively on the set $\Omega \setminus \{0,1\}$, because 2 could be map into any other point:

$$2^{id} = 2,$$
$$2^{(23)(75)(49)(68)} = 3,$$
$$2^{(2439)(5678)} = 4,$$
$$2^{(2537)(4896)} = 5,$$
$$2^{(2638)(7459)} = 6,$$
$$2^{(2735)(4698)} = 7,$$
$$2^{(2836)(4795)} = 8,$$
$$2^{(2934)(5876)} = 9.$$

Hence the Mathieu group M_{10} is sharply 3-transitive. □

5.8 THE CONSTRUCTION OF THE MATHIEU GROUP M_{11}

We are going to construct a one-point extension of the group M_{10} using Theorem 2.2. For this purpose let

$$G = M_{10}, \quad * = T, \quad h = (0T)(47)(59)(68), \quad g = \psi.$$

Question 5.9 [1, 1.9.8] *Show that* $G_0 = \langle \theta, \phi_1, \phi_2, \lambda \rangle$ *and verify that all conditions (i)-(iv) of Theorem 2.2 hold, so that* $\langle M_{10}, h \rangle$ *is sharply* 4*-transitive on the set* $X' = \{0, 1, ...9, T\}$.

Solution. The elements g and h decompose as

$$g = (01)(49)(56)(78) \text{ and } h = (0T)(47)(59)(68).$$

We verify that all conditions (i)-(iv) of Theorem 3.2 hold:

(i): Taking $\alpha = 0$, obviously, the element $h = (0T)(47)(59)(68)$ switches $*$ and α.

(ii): Taking $\beta = 1$, obviously, the element $g = (01)(49)(56)(78)$ switches α and β.

(iii): $h^2 = (0T)(47)(59)(68) \cdot (0T)(47)(59)(68) = id$, so $h^2 \in G$. We also have to prove that $(gh)^3 \in G$. It is true since $g \cdot h = (01T)(458)(697)$, hence $(gh)^3 = id \in G$.

(iv): The last condition is $hG_0h = G_0$. Since we know a generator set of G_0 we could directly check this property:

$$\begin{aligned}
h\phi_1 h &= (0T)(47)(56)(68)(194)(285)(376)(0T)(47)(56)(68) = (483)(715)(926) = \lambda\phi_2\lambda^{-1} \\
h\phi_2 h &= (0T)(47)(56)(68)(123)(456)(798)(0T)(47)(56)(68) = (456)(798)(123) = \phi_2, \\
h\theta h &= (0T)(47)(56)(68)(2934)(5876)(0T)(47)(56)(68) = (4896)(7253) = \lambda^{-1}, \\
h\lambda h &= (0T)(47)(56)(68)(2735)(4698)(0T)(47)(56)(68) = (4392)(7856) = \theta^{-1}.
\end{aligned}$$

For all elements s from the generating set $S = \{\phi_1, \phi_2, \theta, \lambda\}$, hsh is again in G_0, and this proves that $hG_0h = G_0$.

We can conclude that $\langle M_{10}, h\rangle$ is sharply 4-transitive since the order of this group is

$$|\langle M_{10}, h\rangle| = 11 \cdot |Stab_G(0)| = 11 \cdot |M_{10}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7920.$$

□

Definition 5.10 *The group $M_{11} = \langle M_{10}, h\rangle$ constructed above is called the Mathieu group on 11 symbols.*

5.9 THE CONSTRUCTION OF THE MATHIEU GROUP M_{12}

Using Theorem 2.2 once more, we are going to construct a one-point extension of the group M_{11}. For this purpose let

$$G' = M_{11}, \quad * = E, \quad g' = h = (0T)(47)(59)(68).$$

Question 5.11 [1, 1.9.9] *Find a permutation h' of $\{0, 1, ...9, T, E\}$ such that $\langle M_{11}, h'\rangle$ is sharply 5-transitive.*

Solution. We are going to show that by the choice

$$h' = (ET)(49)(56)(78)$$

all conditions (i)-(iv) of Theorem 3.2 hold. Take $\alpha = T$ and $\beta = 0$. Conditions (i) and (ii) hold obviously. Let us check condition (iii): $(h')^2 = id \in G'$, and

$$g'h' = (0T)(47)(59)(68) \cdot (ET)(49)(56)(78) = (0ET)(485)(967),$$

hence $(g'h')^3 = id' \in G'$, and so (iii) holds too.

Condition (iv) requires that

$$h'G'_T h' = G'_T = M_{10} = \langle H, \lambda\rangle = \langle \theta, \phi_1, \phi_1, \lambda, \psi\rangle.$$

Then

$$\begin{aligned}
h'\theta h' &= (ET)(49)(56)(78) \cdot (2934)(5876) \cdot (ET)(49)(56)(78) = (4392)(5678) = \theta^{-1} \\
h'\phi_1 h' &= (ET)(49)(56)(78) \cdot (194)(285)(376) \cdot (ET)(49)(56)(78) = (491)(538)(762) \\
h'\phi_2 h' &= (ET)(49)(56)(78) \cdot (123)(456)(798) \cdot (ET)(49)(56)(78) = (478)(596)(123) \\
h'\lambda h' &= (ET)(49)(56)(78) \cdot (2735)(4698) \cdot (ET)(49)(56)(78) = (4795)(6283) \\
h'\psi h' &= (ET)(49)(56)(78) \cdot (01)(49)(56)(78) \cdot (ET)(49)(56)(78) = (01)(49)(56)(78) = \psi.
\end{aligned}$$

Since it is not obvious that elements $h'\phi_1 h'$, $h'\phi_2 h'$, $h'\lambda h'$ are in G'_T we used program package Magma [3] to check it.

That $\langle M_{11}, h'\rangle$ is sharply 5-transitive follows in the same way as in §5.8.

$$|M_{12}| = 12 \cdot |Stab_{M_{12}}(E)| = 12 \cdot |M_{11}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040.$$

□

Definition 5.12 *The group $M_{12} = \langle M_{11}, h'\rangle$ constructed above is called the Mathieu group on 12 symbols.*

5.10 THE SIMPLICITY OF THE GROUPS M_{11} AND M_{12}

In this section we prove that the two Mathieu groups M_{11} and M_{12} are simple. Let us prove this first for M_{11}.

Theorem 5.13 *The Mathieu group M_{11} is simple.*

Proof. Towards a contradiction let us assume that $N \trianglelefteq M_{11}$ is proper and nontrivial. Since M_{11} is doubly transitive it is primitive. By Theorem 3.5, N is transitive and so 11 divides $|N|$. Let P be a Sylow 11-subgroup of N and s_{11} the number of Sylow 11-subgroups in M_{11}. From Sylow's third Theorem we have that

$$s_{11} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{|N_{M_{11}}(P)|} \text{ and } s_{11} \equiv 1 (\text{mod } 11).$$

This implies that $s_{11} = 144$ and $|N_{M_{11}}(P)| = 55$. Now since $P < N \trianglelefteq G$ and all Sylow 11-subgroups are conjugates, N contains all 144 Sylow 11-subgroups. Using Sylow's third Theorem again we obtain

$$|N| = 144 \cdot N_N(P) = 11 \cdot 2 \cdot 9 \cdot 8.$$

Note that, $N_N(P)$ contains exactly 11 elements since it contains P.

Furthermore, $\frac{|N|}{|N_a|} = 11$ yields $|N \cap M_{10}| \neq 1$, where $M_{10} < M_{11}$ is a point stabilizer of M_{11}. Now, $N \cap M_{10} \trianglelefteq M_{10}$. The group M_{10} acting on $\Omega^+ \setminus \{*\} = \Omega$ is primitive since is it is doubly transitive. This yields that 10 divides $|N \cap M_{10}|$, implying that 10 divides also $|N|$, a contradiction. □

Question 5.14 [1, 1.9.11] *Is M_{10} simple? Assume that M_{11} is simple, and show that M_{12} is simple.*

Solution. The Mathieu group M_{10} is not simple, because it has a subgroup $\hat{A}_6$ of index 2, hence $\hat{A}_6$ is a normal subgroup of the group M_{10}.

Since M_{11} is simple, Lemma 3.6 implies that M_{12} is simple or contains a regular normal subgroup. But M_{12} is a 5-transitive group, then by Theorem 3.9 we can state that M_{12} is simple. □

Chapter 6

SUMMARY

In the master work we have constructed Mathieu groups of the small degree (M_{10}, M_{11}, M_{12}), using methodology of extension, and examined theirs properties. We realized that M_{10}, M_{11}, M_{12} are all primitive groups, because they are all more then 2-transitive. Also we have checked if the groups are simple by simplicity criteria and concluded that M_{10} is not simple, since it has normal subgroup A_6, but M_{11} and M_{12} are simple k-transitive where $k \geq 4$. All these properties are very important, because automorphism groups of many combinatorial and geometrical structures are Mathieu groups, so we could get some useful information from these results.

In general during investigation of multiply transitive groups we have concluded that they are very interesting object for research and also excellent tool for study others areas of mathematics. We tried to show this fact by chapter 3, where we have write some unusual applications of affine and Mathieu groups. For example Mathieu group M_{12} could be used by composers like Olivér Messiaen, he got new melodies by applying permutations from the M_{12} to the 7 notes and 5 diesis. Young mathematician Paul Siegel constructed permutation puzzle by using multiply transitive groups M_{12}, M_{24} and Co_0. And finally classical application of multiply transitive groups like automorphism group of Steiner system.

Bibliography

[1] N. L. Biggs and A. T. White, *Permutation groups and combinatorial structures,* Cambridge University Press, Cambridge 1979.

[2] D. Benson, *Music: a mathematical offering*, Cambridge University Press, Cambridge, 2007.

[3] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: the user language, *Journal of Symbolic Computation* **24** (1997), 235-265.

[4] P. J. Cameron, *Permutation groups*, Cambridge University Press, Cambridge, 1999.

[5] H. S. M. Coxeter, *Introduction to geometry*, Second ed. John Wiley Sons, New York, 1969.

[6] H. Cuyper, *The Mathieu groups and designs*, Available 05.07.2012 on: http://www.win.tue.nl/ hansc/eidmamathieu.pdf.

[7] A. Devillers, M. Giudici, C.H. Li, C. E Praeger, *A remarkable Mathiue graph tower*, Available 05.07.2012 on: http://homepages.ulb.ac.be/ adevil/doc/M11graph.pdf.

[8] J. D. Dixon, B. Mortimer, *Permutation Groups*, Springer, New York, 1996.

[9] A. A Ivanov, *Geometry of sporadic groups I: Petersen and tilde geometries*, Cambrige University Press, Cambrige, 1999.

[10] I. Kriz, P. Siegel, Simple groups at play, *Scientific American* **299** (2008), 84-89.

[11] I. Kriz, P. Siegel, *The puzzle* M_{12}, Available 19.08.2011 on: *http://www.scientificamerican.com/media/inline/2008-07/puzzles/m12.html.*

[12] I. Kriz, P. Siegel, *The puzzle* M_{24}, Available 19.08.2011 on: *http://www.scientificamerican.com/media/inline/2008-07/puzzles/m24.html*.

[13] J. H. Kwak, M. Y. Xu, *Finite group theory for combinatorisist*, Available 05.07.2011 on: http://ishare.iask.sina.com.cn/f/17493716.html.

[14] É. Mathieu, Mémoire sur l'étude des fonctions de plusieurs quantités, sur la maniére de les former et sur les substitutions qui les laissent invariables (in French), *Journal de Mathématiques Pures et Appliquées* **6** (1861), 241-323.

[15] É. Mathieu, Sur la fonction cinq fois transitive de 24 quantités (in French), *Journal de Mathématiques Pures et Appliquées* **18** (1873), 25-46.

[16] C. Nolan, Music theory and mathematics, In: T. Christensen (ed.), *The Cambridge History of Westem Music Theory*, Cambridge Univeristy Press, Cambridge, 2008, 272-304.

[17] E. Ross, *Mathematics and music: The Mathieu group* M_{12}, Available 05.07.2012 on: http://www.lancs.ac.uk/ rosse2/ProjectYr4EmmaRoss.pdf.

[18] J. J. Rotman, *An introduction to the theory of groups*, Springer-Verlag, New York, 1991.

[19] T. Rowland, N. Wedd and E. W. Weisstein, *Transitive Group*, Available 25.08.2011 on: *http://mathworld.wolfram.com/TransitiveGroup.html*.

[20] T. Rowland, N. Wedd and E. W. Weisstein, *Steiner system*, Available 25.08.2011 on: *http://mathworld.wolfram.com/SteinerSystem.html*.

[21] H. Wielandt, *Finite permutation groups*, Academic press, New York, 1964.